AfxLoadLibrary

Vulnerable to "tainted" DLLs placed in a location in the search path before the intended DLL

Sean Barnum, Cigital, Inc. [vita[1]]

Copyright © 2005 Cigital, Inc.

2005-10-03

"Original Cigital Coding Rule in XML"

Mime-type: text/xml, ######: 5661 bytes

Identification Difficulty

Scan

Rule Accuracy

False Positives

Priority

Medium

Attack Categories

- Resource Injection

Vulnerability Categories

- Indeterminate File/Path

Software Context

- Process Management
- File Path Management

Description

AfxLoadLibrary() and CoLoadLibrary() have many implicit, default behaviors that can give an attacker an opportunity to inject object code into your code base. The AfxLoadLibrary() function is used to load code from a DLL library. The system will use ".DLL" for the file extension if it is not specified. If the path for the library to load is not fully qualified, then the system will search the following locations in

1. daisy:35 (Barnum, Sean)

this order: 1. The directory from which the application loaded. 2. The current working directory. (Could be affected by chdir()) 3. The Windows system or system32 directory. On Windows 95/98/Me this is the Windows system directory. On more recent versions of windows it is system32. 4. Windows NT only: The 16-bit Windows system directory. There is no Win32 function that obtains the path of this directory, but it is searched. The default name of this directory is SYSTEM. 5. The Windows directory (typically C:\WINDOWS or C:\WINNT). 6. Each directory listed in the PATH environment variable, in the order they are listed. A somewhat different search strategy is used for CoLoadLibrary(). This issue has reportedly been fixed in Windows XPSP1, Windows Server 2003 and newer versions.

Application Programming Interfaces

Function Name	Comments
AfxLoadLibrary	
CoLoadLibrary	
CoLoadLibraryA	

Method of Attack

An attacker could inject a Trojan horse DLL within your process by placing a "tainted" DLL in a location in the DLL search path that is found before the intended DLL.

Solutions

Applicability	Description	Efficacy
When library is loaded.	The lpszModuleName or lpszLibName parameter should be a fully qualified filename, including the file extension.	Effective if identified file is secure from tampering.

Signature Details

Definite positive signature: call to AfxLoadLibrary() with a literal string that does not begin with "\\" or "[A-Z]:\" Possible positive signature: call to AfxLoadLibrary() with a string or character array variable Definite negative signature:call to AfxLoadLibrary() with a literal string that begins with a drive letter or UNC path (e.g. "\\")

Examples of Incorrect Code

- Example 1

```
AfxLoadLibrary("MyLib");
// or
AfxLoadLibrary("Prog\MyLib.DLL");
```

Examples of Corrected Code

- Example 1

```
AfxLoadLibrary("C:\\Program Files\\MyCompany\\MyProg\\MyLib.DLL");
// or
AfxLoadLibrary("\\\\Server\\Share\\Path\\MyLib.DLL");
```

Recommended Resources

Resource	Link
MSDN reference for AfxLoadLibrary	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclib/html/_mfc_afxloadlibrary.asp[2]
MSDN reference for CoLoadLibrary	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wcedcom/html/cerefcoloadlibrary.asp[3]

Discriminant Set

Operating Systems

- Windows 98
- Windows Me
- Windows 2000
- Windows XP Home
- Windows XP Pro
- Win32

Frameworks

- MFC

Languages

- C
- C++

Attack Agents

- Internal

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005. Cigital-authored documents are sponsored by the U.S. Department of Defense under Contract FA8721-05-C-0003. Cigital retains copyrights in all material produced under this contract. The U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce

2. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclib/html/_mfc_afxloadlibrary.asp
3. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wcedcom/html/cerefcoloadlibrary.asp

these documents, or allow others to do so, for U.S. Government purposes only pursuant to the copyright license under the contract clause at 252.227-7013.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com[1].

####

###	########
Copyright Holder	Cigital, Inc.

####

###	########
Attack Categories	Resource Injection
Operating System	Win32 Windows 2000 Windows 98 Windows ME Windows XP Home Windows XP Pro
Software Context	File Path Management Process Management
Vulnerability Categories	Indeterminate File/Path

1. mailto:copyright@cigital.com